UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/089,506	08/09/2002	William Henry Yost	RCA 89826	9456

7590	03/21/2007
Joseph S Tripoli	
Thomson Multumedia Licensing	
P O Box 5312	
Princeton, NJ 08540	

EXAMINER
ABEDIN, SHANTO

ART UNIT	PAPER NUMBER
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

PTOL-90A (Rev. 10/06)

	Application No.	Applicant(s)
Office Action Summary	10/089,506	YOST, WILLIAM HENRY
	Examiner	Art Unit	
	Shanto M Z Abedin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>03</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>*07 December 2006*</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7* is/are pending in the application.

     4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

     a)☐ All   b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

     * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
     Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
     Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   This office action is in response to the APPEAL BRIEF filed on 12/07/2006.

2.   The examiner withdraws the finality of the previous office action based upon the applicant's

arguments presented in the appeal brief, and this action is made NON-FINAL.

3.   Claims 1-7 are currently presented for the examination.

4.   Claims 1-7 have been rejected.

Priority

5.   The later-filed application must be an application for a patent for an invention which is

also disclosed in the prior application (the parent or original non provisional application or

provisional application). The disclosure of the invention in the parent application and in the later-

filed application must be sufficient to comply with the requirements of the first paragraph of 35

U.S.C. 112. See *Transco Products, Inc. v. Performance Contracting, Inc.*, 38 F.3d 551, 32

USPQ2d 1077 (Fed. Cir. 1994)..

        The disclosure of the prior-filed application, Application No. 60/156385 (filed on

09/28/1999), fails to provide adequate support or enablement in the manner provided by the first

paragraph of 35 U.S.C. 112 for one or more claims of this application. In particularly, claim

limitation such as converting a shared secret into a readable password is not found to be disclosed in

application no 60/156385. Therefore, priority to this application is set to the filing date of the PCT

application, 09/22/2000.

Response to Arguments

6.   Regarding 35 U.S.C 103 (a) rejections of claim 1-7, the applicant primarily argues

followings: (B1) the cited combination of Stallings and StJohns does not teach or suggest converting

the shared secret into a readable password, as recited in claim 1; (B2) the cited combination of

Stallings and StJohns would change the principle of operation of Stallings, thereby making the

teachings of combination not sufficient to render claim 1 prima facie obvious; and (B3) no teaching,

suggestion or motivation exists to combine and/ or modify Stallings and/ or StJohns to produce the

invention claimed in claim 1.

In response to (B1), the applicant's arguments are found persuasive, however they are moot

in view of new grounds of rejections set forth in this office action. In response to the arguments (B2)

and (B3) the examiner respectfully disagrees with the applicant (please see the previous office action

for explanation), however, these arguments are now moot in view of new grounds of rejections.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness

rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior
> art are such that the subject matter as a whole would have been obvious at the time the invention was made to a
> person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived
> by the manner in which the invention was made.

7.   Claim 1-7 are rejected under 35 USC 103 (a) as being unpatentable over StJohns (Diffie-

Hellman Key Change, Internet-draft, 1998) in view of Yu et al (US 6067621) further in view of

Stallings (SNMPv3: A Security Enhancement for SNMP, William Stallings, IEEE, 1998).

Regarding claim 1, StJohns teaches a method for initializing a SNMP (simple network

management protocol) v3 device using an SNMP agent in the SNMPv3 device and SNMP manager

remote from the SNMPv3 device, comprising:

Utilizing a Diffie-Hellman exchange protocol by the SNMP manager and the SNMP agent to

enter an initial privacy key and an initial authentication key into the SNMPv3 device (Page 1, last

paragraph; Page 4, sec 1.1; Page 5, lines 1-3; Diffie-Hellman; authentication and privacy keys),

Wherein said utilizing step includes:

generating an associated random number and public value by both the SNMP manager and

the SNMP agent (Page 6-7; Diffie-Hellman; public values; random integers; usmDHKeyObjects)

passing the public value of the SNMP manager to the SNMP agent in a configuration file

(Page 4, Sec 1.1; usmDHPublicObjects containing DH public parameters)

reading by the SNMP manager, the public value of the SNMP agent through a SNMP request

using an initial valid user having access to the public value of the SNMP agent (Page 6-7; Deffie-

Hellman; exchanging public values;); and

computing a shared secret by the SNMP agent and the SNMP manager, using the Deffie-

Hellman key exchange protocol (Page 7; Diffie-Hellman; computing shared secret, sk);

setting the initial authentication key and the initial privacy key to the value of the secret key

(Page 4, sec 1.1; Page 5, line 1-3; Diffie-Hellman; secret key; updating authentication and privacy

keys).

StJohns fails to disclose

converting the shared secret into a readable password.

converting the readable password into a secret key.

However, Yu et al discloses converting the shared secret into a readable password (Col 9,

lines 1-10; Col 10, lines 1-10; generating password from a shared secret).

StJohns or Yu et al fails to disclose

converting the readable password into a secret key.

However, <u>Stallings</u> discloses converting the readable password into a secret key (Page 12, Col 1, lines 38-48;"secret key" shared by users and authoritative SNMP engine; converting users keys to unique keys; proposal [2]; RFC 2274).

<u>Yu et al</u> , <u>Stallings</u> and <u>StJohns</u> are analogous art because they are from the same field of endeavor of network client authentication and secure key management. At the time of the invention, it would have been obvious to a person of ordinary skill in art to combine the teachings of <u>Yu et al</u> with <u>StJohns</u> to convert the shared secret into a readable password in order to further incorporate an authentication process through one-time/ shared password (Yu et al , Col 9, starting at line 1). At the time of the invention, it would have been further obvious to a person of ordinary skill in art to combine the teachings of <u>Stallings</u> with the modified <u>Yu et al-St Johns</u> system to convert the readable password into a secret key in order to provide a key localization mechanism for further key security (Stallings, page 11-12; key localization).

Regarding claim 2, it is rejected applying as above rejecting claim 1, furthermore, <u>Stallings</u> teaches the method wherein the readable password comprises a 16 character password (Page 12, Col 1, lines 28-37; human-readable passwords; RFC-2274 algorithm for mapping password to key; octet privacy and authentication key; password to key; Page 12, Col 2, lines 25-40; single/ plurality of password to create keys of plurality of bit length).

Regarding claim 3, it is rejected applying as above rejecting claim 1, furthermore, <u>Stallings</u> teaches the method wherein the secret key comprises a 16 byte string (Page 12, Col 1, lines 29-49; Page 13, Col 1, lines 1-10; 16 octet key).

Regarding claim 4, it is rejected applying as above rejecting claim 1, furthermore, <u>Stallings</u>

teaches the method further characterized in the configuration file comprises a proprietary

configuration file element for passing the public value of the SNMP manager to the SNMP agent

(Page 3,Col 2, lines 26- 34; set of documents defining network protocol; proprietary network

management applications; Page 4,Col 2, lines 25-50; Page 9,Col 2, lines 58-66; command generator;

USM files in the security related parameters; authoritative module).

Regarding claim 5, it is rejected applying as above rejecting claim 4, furthermore, <u>Stallings</u>

teaches the method wherein the SNMPv3 device operates in a SNMPv1/ v2c enabled network

comprising a SNMPv2c device (Page 2, Col 2, lines 1-37; SNMPv3 defines a security capability to

be used in conjunction with SNMPv2 or SNMPv1), and wherein the proprietary configuration file

element is ignored by the SNMPv2c device (Fig 1, element : PDU processing for SNMPv1 or

SNMPv2, element: SNMPv3 USM; Table 2, element: snmpSecurityModel; Page 2, Col 2, lines 5-

35; User Security Model (USM) for SNMPv3; SNMP Protocol Data Unit (PDU) for SNMPv1 and

SNMPv2; Page 3, Col 2, lines 25-45; Management Information Base (MIB) for keeping local

configuration data for SNMPv2; *independent configuration/ security or management protocol for*

the different version of SNMP).

Regarding claim 6, it is rejected applying as above rejecting claim 1, furthermore, <u>StJohns</u>

discloses the method wherein the public value of the SNMP manager is included in a management

information base (MIB) object in the configuration file (Page 7; usmDHPublicobjects).

Regarding claim 7, it is rejected applying as above rejecting claim 1, furthermore, <u>StJohns</u>

discloses the method wherein the public value of the SNMP manager is initially stored in a third

entity different from that associated with the SNMP manager and the SNMP agent (Page 1, MIB,

Agent , manager), and the method comprises downloading the configuration from the third entity by

the SNMP agent (Page 9-10; usmUserPrivProtocol; usmDHKeyMIBCompliance; read; installed).

Conclusion

8.   A shortened statutory period for response to this action is set to expire in 3 (Three) months

and 0 (Zero) days from the mailing date of this letter. Failure to respond within the period for

response will result in ABANDOMENT of the application (see 35 U.S.C 133, M.P.E.P 710.02(b)).

Any inquiry concerning this communication or earlier communications from the examiner

should be directed to Shanto M Abedin whose telephone number is 571-272-3551. The examiner

can normally be reached on M-F from 9:00 AM to 5:30 PM. If attempts to reach the examiner by

telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 571-

272-4195. The fax phone number for the organization where this application or proceeding is

assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR system,

see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system,

contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M Abedin

Examiner, AU 2136

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

3/18/07